

● PRINTER RUSH ●

(PTO ASSISTANCE)

Application : <u>09/451254</u>	Examiner : <u>Winter</u>	GAU : <u>3621</u>
From : <u>T. McGill</u>	Location : <u>IDC</u> FMF FDC	Date : <u>9-28-05</u>

Tracking # epm 09/451254 Week Date: 7-25-05

DOC CODE	DOC DATE	MISCELLANEOUS
<input type="checkbox"/> 1449		<input type="checkbox"/> Continuing Data
<input type="checkbox"/> IDS		<input type="checkbox"/> Foreign Priority
<input checked="" type="checkbox"/> CLM	<u>2-24-05</u>	<input type="checkbox"/> Document Legibility
<input type="checkbox"/> IIFW		<input type="checkbox"/> Fees
<input type="checkbox"/> SRFW		<input type="checkbox"/> Other
<input type="checkbox"/> DRW		
<input type="checkbox"/> OATH		
<input type="checkbox"/> 312		
<input type="checkbox"/> SPEC		

[RUSH] MESSAGE: Original claims 5 & 36 (now claims
29) both claims end incomplete,
claim 5 ends with a semi-colon,
claim 36 does not end with a period.
Thank you

[XRUSH] RESPONSE: Corrected the punctuation.

INITIALS: [Signature]

NOTE: This form will be included as part of the official USPTO record, with the Response document coded as XRUSH.
 REV 10/04

1 Claim 3 (Original): A method as recited in claim 1, further comprising
2 storing the stick of electronic assets in an electronic wallet constructed with a
3 secure-processor architecture.

4
5 Claim 4 (Original): A method as recited in claim 1, wherein the minting
6 comprises minting the stick of assets using a blind signature protocol.

7
8 Claim 5 (Original): A method as recited in claim 1, wherein the spending
9 comprises:

10 concatenating a vendor identity with the first asset from the stick to form a
11 payment request;

12 signing the payment request with a signature of the user:

13 submitting the user-signed payment request along with the issuer-signed
14 withdrawal request to the vendor;

15 accepting the first asset as payment in an event that the user and the issuer
16 are verified; and

17 subsequently passing any additional assets from the stick as payment to the
18 vendor without digitally signing them with the user's signature. *J.*

19
20 Claim 6 (Original): A method comprising:

21 minting a stick of electronic assets by digitally signing with an issuer's
22 signature a composite of user-provided data items including a user identity, a
23 bottom asset from a bottom of the stick, and a length of the stick;

24 spending one or more assets from the stick at one or more vendors, wherein
25 each expenditure with a particular vendor involves digitally signing with a user's

signing, at the issuer, the withdrawal request by computing:

$$c = (p^0 C_L)^L = p^L C_L^L \bmod N$$

deriving a new bottom asset by computing:

$$C_L^U = c/p^L \bmod N.$$

Claim 36 (Original): A method as recited in claim 34, further comprising verifying the bottom asset by computing C_L^H independently and comparing a result to the new bottom asset derived in said deriving (C_L^H).

Claim 37 (Original): A method as recited in claim 34, further comprising storing the blind stick of electronic assets and signed withdrawal request in an electronic wallet constructed with a secure-processor architecture.